

CofC

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE



Applicant(s): John B. Beavers

Assignee: Symantec Corporation

Title: SYSTEM AND METHOD FOR TRACKING AND FILTERING
ALERTS IN AN ENTERPRISE AND GENERATING ALERT
INDICATIONS FOR ANALYSIS

Serial No.: 10/080,574 Filing Date: February 25, 2002

Patent No.: 7,171,689 Issued: January 30, 2007

Examiner: Nirav B. Patel Group Art Unit: 2135

Docket No.: SYMC1023

Monterey, CA
February 20, 2007

ATTENTION: CERTIFICATE OF CORRECTIONS BRANCH
COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA. 22313-1450

REQUEST FOR ENTRY OF
CERTIFICATE OF CORRECTION

Certificate
FEB 28 2007
of Correction

Sir:

Please enter the enclosed Certificate of Correction (PTO Form 1050) in the above patent.

The errors sought to be corrected were made by

☒ The Patent and Trademark Office as explained below. Thus, no fee is required for the Certificate of Correction pursuant to 37 CFR §1.322.

☐ Applicant(s) (at least in part). See next section for explanation. This appropriate fee under 37 CFR §1.323 has been authorized below.

MAR - 1 2007

Attached as Exhibit A (2 pages) is a copy of the relevant pages of the Proposed Claim Amendments as submitted to the U.S. Patent and Trademark Office via facsimile on August 17, 2006. Attached as Exhibit B (2 pages) is a copy of the relevant pages of the Examiner's Amendment which was mailed to Applicants with

the Notice of Allowance on August 24, 2006. These Exhibits support the requested correction to Claim 14, and show that the error was made by the U.S. Patent and Trademark Office.

As shown in Exhibit A, Line 19 of originally numbered Claim 15 (renumbered in the Patent as Claim 14) reads "identifying a message type from a plurality of message types". The same line in the patent at Column 18, Line 64 reads "identifying a message type from a plurality message types".

This error was first introduced in the Examiner's Amendment, submitted as Exhibit B.

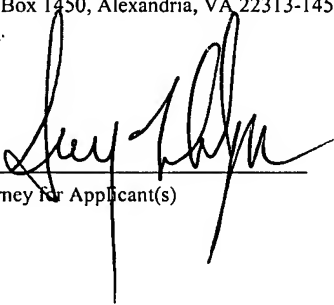
In light of these Exhibits, Applicants respectfully request that the enclosed Certificate of Correction (PTO form 1050) be entered in the above patent.

The Commissioner is hereby authorized to charge any fees required for consideration and entry of the enclosed documents, and to credit any overpayment of fees to Deposit Account No. 50-0553.

Please direct all inquiries concerning this request to the undersigned attorney.

CERTIFICATE OF MAILING

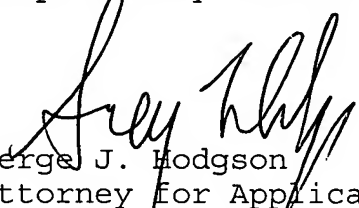
I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on February 20, 2007.



Attorney for Applicant(s)

February 20, 2007
Date of Signature

Respectfully submitted,



Serge J. Hodgson
Attorney for Applicant(s)
Reg. No. 40,017
(831) 655-0880

MAR - 1 2007

12. (Original) The method of claim 11, wherein the rule requires that each output occur a number of times over a period of time before an alert indication is generated.

13. (Canceled)

14. (Currently amended) The method of claim ~~13~~ 1, wherein a threat level is included as part of the alert indication.

15. (Currently amended) A system for producing at least one alert indication based on a number of events derived from an enterprise comprising:

a plurality of enterprise devices, each device capable of producing an output;

a number of translation files, the translation files allowing the output to be translated into a common format event, the translation comprising:

matching data values in the device output with a signature specification for each enterprise device, the signature specification containing:

a number of signatures;

a first location identifier for each signature; and

a first key;

wherein the signature is a listing of names found in the device output, the first location identifier determines how to

locate the name in the device output, and the first key determines where to locate the name in the device output;

identifying a message type from a plurality of message types for each enterprise device based on the device output as part of the translated common format event;

a number of knowledge base table files, matching of the common format event with one or more of the knowledge base table files adding knowledge from the matched file to generate a knowledge-containing common format event;

a number of rule files, the rule files governing generation of the alert indication; and

a rules processor for generating the alert indication, wherein the alert indication includes at least a text message describing the event contained in the output of the enterprise device.

16. (Original) The system of claim 15, wherein the enterprise devices are selected from the group consisting of a server, a firewall, a modem, a work station, a router, a remote machine, an intrusion detection system, an identification and authentication server, network monitoring and management systems, network components, and one or more combinations thereof, or any generator of data streams on the computer network.

argument value, and the second key locates the argument value in the device output to be displayed with the argument name.

d. Referring to claim 13:

Please cancel claim 13.

e. Referring to claim 14:

Please replace claim 14 as follows:

The method of claim 1, wherein a threat level is included as part of the alert indication.

f. Referring to claim 15:

Please replace claim 15 as follows:

A system for producing at least one alert indication based on a number of events derived from an enterprise comprising:

a plurality of enterprise devices, each device capable of producing an output;

a number of translation files, the translation files allowing the output to be translated into a common format event, the translation comprising:

matching data values in the device output with a signature specification for each enterprise device, the signature specification containing:

a number of signatures; a first location identifier for each signature; and

a first key;

MAR - 1 2007

MAR - 1 2007

MAR - 1 2007

Exhibit B

wherein the signature is a listing of names found in the device output, the first location identifier determines how to locate the name in the device output, and the first key determines where to locate the name in the device output;

identifying a message type from a plurality message types for each enterprise device based on the device output as part of the translated common format event;

a number of knowledge base table files, matching of the common format event with one or more of the knowledge base table files adding knowledge from the matched file to generate a knowledge-containing common format event;

a number of rule files, the rule files governing generation of the alert indication; and

a rules processor for generating the alert indication, wherein the alert indication includes at least a text message describing the event contained in the output of the enterprise device.

Response to Arguments

3. Applicant's arguments, filed June 05 2006 have been fully considered and are persuasive.

Allowable Subject Matter

4. Claims 1-12 and 14-22 are allowed.

MAR - 1 2007

UNITED STATES PATENT AND TRADEMARK OFFICE CERTIFICATE OF CORRECTION

PATENT NO : 7,171,689

Page 1 of 1

APPLICATION NO. : 10/080,574

DATED : January 30, 2007

INVENTOR(S) : John B. Beavers

It is certified that an error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In Column 18, Line 64, Claim 14, between "plurality" and "messages" insert --of--.

MAILING ADDRESS OF SENDER (Please do not use customer number below):

GUNNISON, McKAY & HODGSON, L.L.P.
1900 Garden Road, Suite 220
Monterey, CA 93940

This collection of information is required by 37 CFR 1.322, 1.323, and 1.324. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1.0 hour to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Attention Certificate of Corrections Branch, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2

MAR - 1 2007